REMARKS

Amendments have been made to the Title and specification. Claims 1, 6, 13, 18, 25, 30, 39, and 44 have been amended. No new matter has been introduced with these amendments, all of which are supported in the specification as originally filed. Claims 3 - 5, 15 - 17, 27 - 29, and 41 - 43 have been cancelled from the application herein without prejudice. Claims 1 - 2, 6 - 7, 9 - 14, 18 - 19, 21 - 26, 30 - 32, 34 - 37, 39 - 40, 44 - 45, and 47 remain in the application.

I. Objection to the Title

Paragraph 2 of the Office Action dated March 4, 2005 (hereinafter, "the Office Action") states that the Title is objected to as not being descriptive. The Examiner suggests prepending "Method, System, and Computer Program Product" to the current Title. The MPEP states, in §606.11, "Examiner May Require Change in Title", that "This [changing the title] may result in slightly longer titles, but the loss in brevity of title will be more than offset by the gain in its informative value in indexing, classifying, searching, etc.". Applicant respectfully submits that adding the suggested terms to the current Title will in no way provide a "gain in ... informative value [for] indexing, classifying, [or] searching". However, to avoid further delay in passing the application to issuance, Applicant has amended the Title as per the Examiner's suggestion, and the Examiner is therefore respectfully requested to withdraw this objection.

II. Objection to the Claims

Paragraph 9 of the Office Action states that Claims 5 - 6, 17 - 18, and 29 - 30 are objected to because of their numbering. In view of the amendments and cancellations made herein, this objection is rendered moot, and the Examiner is therefore respectfully requested to withdraw the objection.

III. Rejection under 35 U.S.C. §102(b)

Paragraph 12 of the Office Action states that Claims 13 - 19, 21 - 22, 24 - 33, 34 - 35, 37, 39 - 45, and 47 are rejected under 35 U.S.C. §102(b) as being anticipated by Patel et al ("An Efficient Discrete Log Pseudo Random Generator"). Claims 15 - 17, 27 - 29, and 41 - 43 have been cancelled from the application without prejudice, rendering the rejection moot as to those claims. This rejection is respectfully traversed with regard to the remaining claims.

Applicant's independent Claims 13, 25, and 39 (as well as Claim 1) have been amended herein to incorporate limitations from now-cancelled dependent claims, by way of clarification. Applicant's independent claims explicitly specify that the <u>C-bit input value</u> is provided "as an exponent of" the 1-way function (see Claim 1, lines 6 - 8, referring to "a length in bits, C, of the input value" and "using the provided input value as an exponent of a 1-way function"). These independent claims further specify that the "base of the modular exponentiation is a fixed generator value" (see Claim 1, line 9).

With reference to Claim 16, which previously contained the limitation pertaining to use of the input value as an exponent, the Office Action cites Patel, page 313, section 5, line

10. However, what is stated therein is use of an exponent x_i and using, as output of an i^{th} step, a subset of the bits of x_i. In particular, the lower $n - \omega(\log n)$ bits of x_i are used as output. In other words, the size of Patel's exponent is *n* bits. By contrast, Applicant's claimed invention uses a C-bit exponent.

With reference to Claim 17, which previously contained the limitation pertaining to the "fixed generator value", the Office Action cites Patel, page 304, section 1, line 3 - 4. However, Applicant respectfully notes that what is specified therein is "a generator of the cyclic group of non zero elements in the finite field", not a fixed generator value.

Accordingly, Applicant respectfully submits that his independent Claims 1, 13, 25, and 39 are patentable over the teachings of Patel. Dependent Claims 14, 18 - 19, 21 - 22, 24, 26, 30 - 33, 34 - 35, 37, 40, 44 - 45, and 47 are therefore deemed patentable over the reference as well. The Examiner is therefore respectfully requested to withdraw the §102 rejection.

IV. Rejection Under 35 U.S.C. §103(a)

Paragraph 30 of the Office Action states that Claims 23 and 36 are rejected under 35 U.S.C. §103(a) as being unpatentable over Patel in view of Schneier ("Applied Cryptography"). Paragraph 31 - 32 of the Office Action state that Claims 1 - 7 and 9 - 12, respectively, are also rejected using these references. Claims 3 - 5 have been cancelled from the application without prejudice, rendering the rejection moot as to those claims. These rejections are respectfully traversed with respect to the remaining claims.

Applicant's amendments to independent Claim 1 have been discussed above, and Applicant respectfully submits that this claim is patentable over Patel and/or Schneier. Dependent Claims 2, 6 - 7, and 9 - 12 are therefore deemed patentable over the references as well. Dependent Claims 23 and 36 are deemed patentable by allowability of the amended independent claims from which they depend (which were addressed above). The Examiner is therefore respectfully requested to withdraw the §103 rejection.

V. Conclusion

Applicant respectfully requests reconsideration of the pending rejected claims, withdrawal of all presently outstanding objections and rejections, and allowance of all remaining claims at an early date.

Respectfully submitted,

Marcia L. Doubet

Marcia L. Doubet
Attorney for Applicant
Reg. No. 40,999

Customer Number for Correspondence: 43168
Phone: 407-343-7586
Fax: 407-343-7587